REMARKS

Applicant appreciates the Examiner's thorough examination of the present application as evidenced by the Office Action of January 11, 2006 (hereinafter "Final Action"). Applicant especially appreciates the indication that Claims 4, 5, 8, 9, 19, 20, 23, 24, 28, 29, 32, and 33 recite patentable subject matter. In response, Applicant has amended independent Claims 1, 16, and 25 to clarify that the stream cipher comprises a logical combination of the random values and plaintext. Applicant respectfully submits that the cited reference fails to disclose or suggest, among other things, all of the recitations of independent Claims 1, 16, and 25. Accordingly, Applicant submits that all pending claims are in condition for allowance. Favorable reconsideration of all pending claims is respectfully requested for at least the reasons discussed hereafter.

Previous Amendment

In Applicant's October 3, 2005 response, dependent Claims 3, 7, 18, 22, 27, and 31 were to clarify that the values of the counters are utilized in determining the at least two sequential random values. The Final Action states that no amendments were identified by Applicant. This is because the underlining of the word "in" before "determining" is difficult to detect in the amended claims. Applicant respectfully submits that Claims 3, 7, 18, 22, 27, and 31 were amended in October 3, 2005 response and that the amended claims satisfy the requirements of 35 U.S.C. §112.

Section 112 Rejections

Dependent Claims 2 - 9 and 17 - 33 stand rejected under 35 U.S.C. §112 as being indefinite. In response, Applicant has amended independent Claims 1, 16, and 25 to remove the recitation "for the stream cipher." As a result, the antecedent basis errors have been removed.

Section 101 Rejections

Independent Claims 1 and 25 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. As discussed in the Manual Of Patent Examining Procedure (MPEP):

> The claimed invention as a whole must accomplish a practical application. That is, it must produce a "useful, concrete and tangible result." *State Street*, 149F.3d at 1373, 47 USPQ2d at 1601-02. The purpose of this requirement is to limit patent protection to inventions that possess a certain level of "real world" value, as opposed to subject matter that represents nothing more than an idea or concept, or is simply a starting point for future investigation or research....
>
> [T]he following [example illustrates a] claimed [invention] that [has] a practical application because [it produces] useful, concrete, and tangible result: ...
>
> -"[T]ransformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces 'a useful, concrete and tangible result' -- a final share price momentarily fixed for recording and reporting purposes and even accepted and relied upon by regulatory authorities and in subsequent trades." State Street, 149 F3d at 1373, 47 USPQ2d at 1601....

MPEP, Sec. 2106(II.)(A.), page 2100-6, cols. 1-2. (Underline added) As further discussed in the MPEP:

> Office personnel have the burden to establish a *prima facie* case that the claimed invention as a whole is directed to solely an abstract idea or to manipulation of abstract ideas or does not produce a useful result. Only when the claim is devoid of any limitation to a practical application in the technology arts should it be rejected under 35 U.S.C. Sec. 101. ...
>
> An applicant may assert more than one practical application, but only one is necessary to satisfy the utility requirement.

MPEP, Sec. 2106(II.)(A.), page 2100-7, col. 1. (Underline added.)

Claims 1 and 25 have been amended to indicate the stream cipher comprises a logical combination of the random values and plaintext. As is well known to those of skill in the art of cryptography, a stream cipher is a symmetric cipher in which plaintext digits are encrypted one at a time, and in which the transformation of successive digits varies during the encryption. As discussed on page 1 of the Specification, the cipher text can be encrypted and decrypted by XORing the plaintext/cipher text with the random values. Applicant respectfully submits that a stream cipher generated using random values is a useful, concrete, and tangible result in the field of cryptography. Applicant submits that the stream cipher generated using random values determined using a common S-box is at least as useful, concrete, and tangible as the final share price used by regulatory authorities and in subsequent trades described in the State Stree decision cited above. In addition, Applicants submit that

Claims 1 and 25 are not devoid of any limitation to a practical application in the technology arts as set forth above.

Accordingly, Applicants respectfully submit that Claims 1 and 25 meet all the requirements of 35 U.S.C. §101.

Section 103 Rejections

Independent Claims 1, 16, and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 6,490,354 to Venkatesan et al. (hereinafter "Venkatesan") in view of U. S. Patent No. 5,434,807 to Yoshida (hereinafter "Yoshida"). (Final Action, page 7). Independent Claims 1, 16, and 25 are directed to a method, system, and computer program product for determining random values for a stream cipher in which at least two sequential random values are determined in parallel using a common S-box.

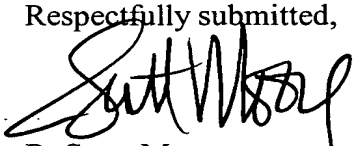
Venkatesan describes a keystream generator in which procedure 620 of FIG. 6 is iteratively executed to generate a continuous pseudo-random word sequence. (See, e.g., Venkatesan, col. 10, lines 35 - 41). The Final Action acknowledges that Venkatesan does not disclose or suggest determining at least two sequential random values in parallel, but maintains that Yoshida provides the missing teachings. Applicant respectfully disagrees as Yoshida describes the generation of random patterns using an n-stage shift register. Yoshida does not appear to have any teaching with respect to generating sequential random values in parallel using a common S-box. Thus, Applicant submits that there would be no motivation to combine the teachings of Venkatesan and Yoshida as they different techniques to generate random values/patterns (S-box Venkatesan and shift register in Yoshida). Moreover, even if the disclosures of Venkatesan and Yoshida were to be combined, neither reference discloses or suggests determining random values for a stream cipher in which at least two sequential random values are determined in parallel using a common S-box.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that independent Claims 1, 16, and 25 are patentable over Venkatesan and Yoshida, and that Claims 2 - 9, 17 - 24, and 26 - 33 are patentable at least as they depend from an allowable claim.

CONCLUSION

In light of the above remarks, Applicant respectfully submits that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,



D. Scott Moore
Registration No. 42,011

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer Number **20792**

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on April 11, 2006.

Traci A. Brown